Ransomware Relies on Poor Data Access Governance

Protection through Containment

In modern building construction, firewalls are put in place to contain the effects of a fire that might break out in a given area. The idea is that if the fire can be contained to a specific section, then despite the damage, you won't lose the building.

Think of ransomware as a fire that you must be prepared to fight. What can you do to contain ransomware using a similar approach?

Data Access Governance (DAG) is all about controlling insider access to data using concepts such as least privilege and separation of duties. The mention of insider access conjures images of employees doing bad things. Worse, however, is the attitude, "Sure, there are bad apples in every barrel, but our people are good people." This is the type of thinking that relegates DAG to an organization's "nice-to-have" list.

Astute security leaders know that the easiest way for outsiders to gain access to their organization's data is through insider access. Compromised credentials and Trojan horses (phishing) are the most common tactics. Data exfiltration (where the bad guys can publish your secrets) and ransomware continue to make headlines. If you don't take precautions against these threats, before you know it, the "building" is on fire.

Identifying What Needs Protecting

Which files need the most protection? Sure, you can get in trouble by not adequately protecting compliance-related data such as

PII, PCI, or PHI. Those file types are definitely important. But ask the CEOs at Colonial Pipeline and JBS Foods what landed them on the evening news? And, in the case of the former, in front of Congress? The lesson is clear: If you don't protect the "crown jewels," you will find yourself poorer, severely wounded, or out of business faster than you can say, *"It won't happen to me."* It *will* happen to you and it's only a matter of time. Based on the principles of well-known security frameworks such as Gartner's CARTA and the NIST Cybersecurity Framework, both Colonial Pipeline and JBS could be hit again. Will they be prepared? Will *you* be prepared if your organization is the target instead?

Too Much Access: A Disaster Waiting to Happen

Some look to encryption as a protection from ransomware. Data encryption can help,

- Can you verify that the files you consider the "crown jewels" of your organization are stored in locations with restricted access permissions?
- What would happen if these files were compromised through ransomware?
- Can you easily conduct a least-privilege analysis of employee access permissions?
- Are you conducting regular access reviews?

but it's no silver bullet. For example, many times the ransomware attack vector involves the employee's own machine, which holds the decryption keys for seamless day-to-day access. Furthermore, even if you happen to be attacked in a way other than through the machine that holds the keys, data encryption really only helps with the threat of exfiltration. It doesn't keep the bad guys from locking you out of your own data.

Even though there are no silver bullets, there is an arsenal. Along with the usual measures of user education and patching, we really need to talk about DAG (and related technology such as Privileged Access Management or PAM) for correcting the real problem of over exposure. Use of these technologies can significantly mitigate the scope and extent of ransomware and similar types of attacks.

Like a fire in a building, ransomware is only as destructive as the access it is able to gain into the network.

Think of your organization's data footprint as the floorplan of a building as shown in Figure 1. Data for certain purposes and sets of people are located in certain areas.

Identity and Role

Want to stop the bad guys? Stop giving them what they are counting on: a hunting ground with few or no data firewalls. Full network access, whether it's granted to the administrative assistant or the CEO, is a disaster waiting to happen. Do either of them *really* need access to everything? No!

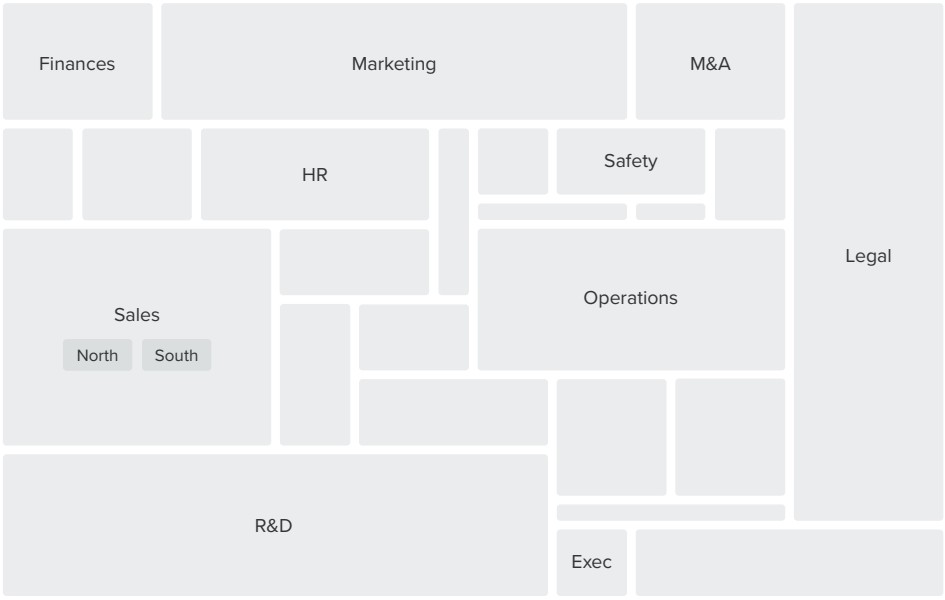

Figure 1. Comparable to a building floorplan, data for certain purposes and sets of people are located in certain areas of the network.

That's why the viability of *identity* and *role* as key factors in securing data is undisputed. Security is really about the right people having the right access to the right data in the right place at the right time. Most of these "rights" are defined by role—and role is articulated through identity.

Taking Focused Corrective Actions

Fortunately, you don't have to boil the ocean to take corrective measures. You can do so by putting a few firewalls in your "building" as shown in Figure 2. Security analysts recommend that you:

- Use a phased approach.
- Start with the "crown jewels" or "High-Value Targets." Examples include storage locations of financial, legal, and confidential proprietary files. You already know where this data is, or at least where it is supposed to be.

For each High-Value Target, you should:

1. Do an analysis of access and remediate using the concepts behind least privilege, restricting user access to the minimum levels needed to perform job functions.
2. Defend against access escalation and entropy by putting automation policies in place to lock down access so that it doesn't change; or at least allow it to change only within certain limits.
3. Perform periodic access reviews to continually ensure that only the people who really need access have it.

That's DAG.

As you move forward, you'll have a "building" with a data footprint like this:

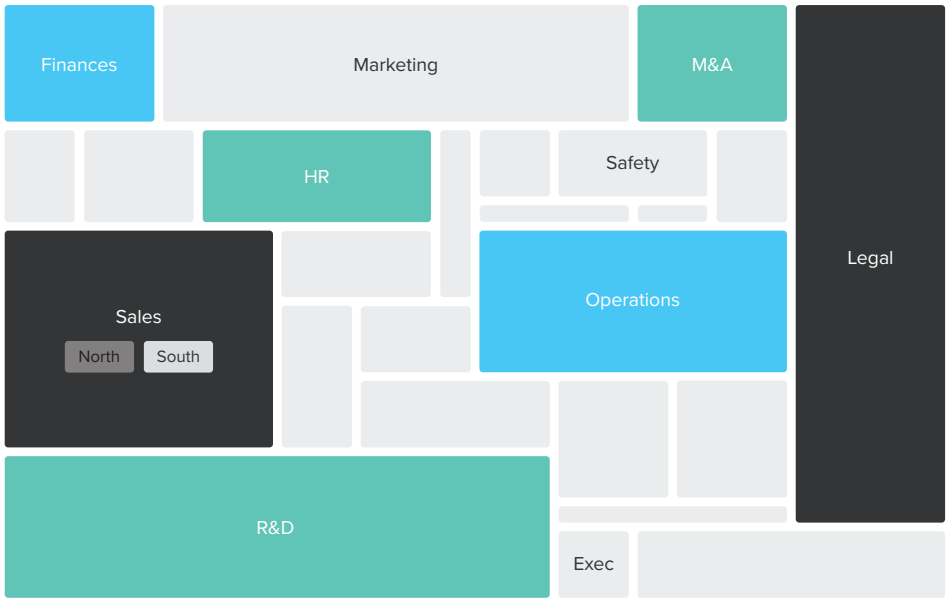

Figure 2. Similar to constructing firewalls that limit the spread of a fire to a room, protecting High-Value Targets through least privilege access limits the capability of ransomware to spread across a network.

With protection like this, a phishing attack sent through email to the administrative assistant of the South Region of Sales is limited to the user's least-privilege access—effectively limiting it to the utility closet" of the "building." Likewise, even a successful attack through the VP of Sales restricts the effects to a single "room" while saving the "building."

DAG Product Offerings

Data Access Governance is an emerging market segment that focuses on identifying and addressing the malicious and non-malicious threats that can come from unauthorized access to sensitive and valuable unstructured data. Many software companies have developed and introduced DAG products with the objective of securing and protecting network-stored unstructured data from unauthorized access, data breaches, and data loss.

NetIQ Data Access Governance offers an enterprise DAG solution *built on identity and role*. It is engineered to integrate with IAM systems—providing application-based data access management and NetIQ Identity Governance to deliver access reviews for unstructured data.

Learn more at
www.microfocus.com/en-us/cyberres/identity-access-management/access-governance

Contact us at **CyberRes.com**
Like what you read? Share it.

CyberRes
A Micro Focus Line of Business